UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/763,621 | 04/26/2001 | Harald Vater | JEK/YATER | 8124 |

23364 7590 11/13/2006

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

| EXAMINER | |
|---|---|
| COLIN, CARL G | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2136 | |

DATE MAILED: 11/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**



Application Number: 09/763,621
Filing Date: April 26, 2001
Appellant(s): VATER ET AL.

Benjamin E. Urcia
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed August 17, 2006 appealing from the Office action mailed on November 16, 2005.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| US 2001/0053220 A1 | KOCHER ET AL | 12-2001 |

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication US 2001/0053220 to Kocher et al. This rejection is set forth in a prior Office Action mailed on November 16, 2005.

As per claim 1, Kocher et al discloses a data carrier having a semiconductor chip (see abstract) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that,
as interpreted by the Examiner, the standard DES, S look up (with no blinding), in Kocher et al meets the recitation of operation h, and a blinded S table meets the recitation of a disguised operation (see paragraph 11); Kocher et al discloses blinded S table, the S tables themselves are stored in blinded form using XOR operation and random values (disguised operation) before the S table lookup operation (before execution) to obtain a disguised lookup table (disguised operation) different than the standard S table in standard DES (without blinding) that meets the recitation of the operation (h) is disguised before its execution, to obtain a disguised operation (h $R_1$) that is a different operation than the operation (h) (see paragraph 11); (see also page 10, claim 37, disclosing transformed table as a disguised table); Kocher et al further discloses the input data A and B are also blinded (disguised) for table look up operation using the blinded S table (disguised operation) that meets the recitation of the disguised operation is executed with disguised input data (see paragraph 11); Kocher et al also discloses that the ciphertext produced by using disguised look up table with disguised input data is equivalent to the ciphertext produced by the standard DES operation (look up table operation without blinding) that meets the recitation of the disguising of the operation (h) and the input data (x) is coordinated such that

the execution of the disguised operation (h $R_1$) with disguised input data yields output data (y) identical with the output data (y) determined upon execution of the operation (h) with input data (x) (see paragraphs 11 and 65; and page 4, paragraph 36), (see also end of claim 37, last step (e) first two paragraphs); whereby disguising operation (h) prevents analysis of said operation (h) and exposure of secret information about said semiconductor chip should a potential attacker intercept signal patterns generated during execution of said disguising operation (h $R_1$), (see paragraphs 9, 11, and 52), in which Kocher et al teaches that blinding the tables and the input data make the state information in the cryptographic processing and the operations unpredictable to attackers and any correlation to secret information is partially or completely hidden, as a result it is impossible for attackers to determine secret parameters through analysis of leaked information from the semiconductor chip device.

**(10) Response to Argument**

Appellant's arguments about Kocher et al, hereafter Kocher, not disclosing a disguised operation are not persuasive. Applicant's specification page 4, lines 22 et seq. provided by Appellant in the summary of claimed subject matter of claim 1, for disclosing the claimed invention describes a look up table representing (function h) or (operation h). Figure 3b shows an example of a disguised look up table (disguised operation) derived from the look up table (operation h) by manipulating only the input data (Xoring the values of the first line) to obtain a disguised look up table (disguised operation) different than look up table (operation h) in figure 3a. According to this example, the look up table or operation (figure 3b) is disguised because the input values (secret data) are hidden with the XOR function applied only to the input values as

recited on page 5, lines 8-9, which states, "The table shown in figure 3b could already be used as a disguised lookup table for processing secret data likewise disguised with random number R1=11." It appears that on page 10 of the appeal brief filed on August 17, 2006, Appellant concedes that Kocher disguises the input data to obtain the same ouput values, which means that Kocher discloses the disguised operation of claim 1 as explained above in light of Applicant's specification. In response to Appellant's arguments on page 10, last two lines to page 11, "Kocher does not disclose that both the input data and an operation performed on the input data resulting in a different operation being applied to the different input data, it is noted that the features upon which applicant relies in this statement are not recited in the rejected claim(s). See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner asserts as shown in the rejection of claim 1 above that Kocher discloses blinding (XOR operation with random values) both the input data and the S tables as disclosed in paragraph 12 of Kocher. Kocher, paragraph 52, further recites "Randomizing blinds the data bit values in this embodiment through an XOR operation... To avoid correlation attacks, an XOR table is constructed with the value to XOR..." Claim 37 of Kocher discloses deriving a transformed representation of said lookup table from the received lookup table as table lookup operation. In Kocher, a blinding operation may be performed as a XOR operation. Therefore, in Kocher a disguised operation is obtained by XORing the table with random values and/or XORing the secret data with random values. In claim 1 of Applicant's invention, a disguised operation may be obtained by only XORing the secret data with random values (as shown in applicant's specification figures 3a-3b; figure 3b is the same as figure 3c).

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

GC

CC

Conferees:

Gilberto Barron

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Benjamin Lanier

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314